IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

Inventor:	Peter Kleinschmidt
Application No.:	10/681,266
Filed:	October 9, 2003
Title:	PERSONAL ELECTRONIC WEB HEALTH LOG
Examiner:	Evens J. Augustin
Art Unit:	3621

APPEAL BRIEF

May It Please The Honorable Board:

Appellants appeal the Rejection, dated April 20, 2007 of Claims 1-18 of the above-identified application. The fee of five hundred dollars ($500.00) for filing this Brief is to be charged to the credit card indicated with filing. Enclosed is a single copy of this Brief.

No additional fee is believed due with this response. However, please charge any additional fee or credit any overpayment to Deposit Account 19-2179.

Appellants do not request an oral hearing.

I. REAL PARTY IN INTEREST

The real party in interest of Application Serial No. 10/681,266 is the Assignee of record:

SIEMENS AKTIENGESELLSCHAFT
WITTELSBACHERPLATZ 2
MUNICH, GERMANY D-80333

II. RELATED APPEALS AND INTERFERENCES

There are currently, and have been, no related Appeals or Interferences regarding Application Serial No. 10/681,266.

III. STATUS OF THE CLAIMS

Claims 1-18 are rejected and the rejection of claims 1-18 are appealed.

IV. STATUS OF AMENDMENTS

All amendments were entered and are reflected in the claims included in Appendix I. No amendments were made to the claims after the Final Rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 provides a personal electronic web health log for personal health data associated with a user (Page 2, paragraph 0008). The web health log includes a data interface, usable to set up a communication link to system participants when required in order to transfer data from a local health log to system participants at least intermittently (Page 1, paragraph 0002; Figure 1). The local health log is included on a user's computer with pre-structured electronic forms for inputting the personal health data by system participants (Page 2, paragraph 0008). The web health log also includes a converter for producing anonymous encrypted data permitting no inference of an identity of the user and for communicating said anonymous encrypted data addressed filing of at least a portion of the anonymous encrypted data on a network (Page 2, paragraph 0008). The converter is actuated using selection schemes, including filters, the filters are valid for particular questions associated with the local health log and for marking data in the local health log used for targeted partial forwarding to system participants (Page 6, paragraph 0024; Page 7, paragraph 0030).

Dependant claim 2 includes the features of independent claim 1 along with the additional feature of a user interface, protected by an authentication device, is for inputting and maintaining data (Page 4, paragraph 0015).

Dependant claim 3 includes the features of dependent claim 2 along with the additional feature of the user interface includes at least one of a keyboard and at least one interface to at least one of a card and label readers and a remote controller (Page 4, paragraph 0015).

Dependant claim 4 includes the features of independent claim 1 along with the additional feature of the local health log includes tables with chronological updating, free text fields and link elements (Page 5, paragraph 0016).

Dependant claim 5 includes the features of dependent claim 4 along with the additional feature of the link elements, which allow jumps to other places in the local health log, other documents and Internet addresses, include at least one of, link elements for charts and images, link elements for fax and photo reproductions and e-mails containing documents and connections to doctors, laboratories having further data (Page 5, paragraph 0016).

Dependant claim 6 includes the features of independent claim 1 along with the additional feature of the selection schemes including elements of a consistency check for the purpose of checking the data for obvious errors and inconsistencies (Page 10, paragraph 0039).

Dependant claim 7 includes the features of independent claim 1 along with the additional feature at least one anonymous encrypted health log downstream of the converter and positioned at a storage location on the Internet via an Internet interface, and in which names and communication data for doctors are suppressed as standard and discriminating at least one of illnesses and treatments which are suppressed under the responsibility of the user (Page 10, paragraph 0041).

Dependant claim 8 includes the features of independent claim 1 along with the additional feature of a secure device for filing and finding a pseudonym ID under which the data are filed in encrypted form on the Internet (Page 4, paragraph 0012).

Dependant claim 9 includes the features of dependent claim 8 along with the additional feature of at least one of a web visiting card and emergency ID, stored on the Internet via an authentication device, which contain the pseudonym ID (Page 4, paragraph 0013).

Dependant claim 10 includes the features of independent claim 1 along with the additional feature of a contractual module for transactions on a consumer-oriented health market (Page 2, paragraph 0007; Page 10, paragraph 0042).

Dependant claim 11 includes the features of dependent claim 2 along with the additional feature of the local health log includes tables with chronological updating, free text fields and link elements (Page 5, paragraph 0016).

Dependant claim 12 includes the features of dependent claim 3 along with the additional feature of the local health log includes tables with chronological updating, free text fields and link elements (Page 5, paragraph 0016).

Independent claim 13 provides a personal electronic web health log for personal health data associated with a user (Page 2, paragraph 0008). The web health log includes a data interface, usable to set up a communication link to system participants and adapted to transfer data from the health log to the system participants at least intermittently (Page 1, paragraph 0002; Figure 1). The web health log also includes a user computer having at least a local health log with pre-structured electronic forms for inputting the personal health data (Page 2, paragraph 0008) and a converter. The converter produces anonymous encrypted data permitting no inference of an identity of the user and communicates the anonymous encrypted data addressed filing of at least a portion of the anonymous encrypted data on a network (Page 2, paragraph 0008). The converter is adapted to be actuated using selection schemes, including filters. The filters are valid for particular questions associated with the local health log and for making data in the local health log used for targeted partial forwarding to system participants (Page 6, paragraph 0024; Page 7, paragraph 0030).

Dependant claim 14 includes the features of dependent claim 2 along with the additional feature of a secure device for filing and finding a pseudonym ID under which the data are filed in encrypted form on the Internet (Page 4, paragraph 0012).

Dependant claim 15 includes the features of dependent claim 14 along with the additional feature of at least one of a web visiting card and emergency ID, stored on the Internet via an authentication device, which contains the pseudonym ID (Page 4, paragraph 0013).

Dependant claim 16 includes the features of dependent claim 3 along with the additional feature of a secure device for filing and finding a pseudonym ID under which the data are filed in encrypted form on the Internet (Page 4, paragraph 0012).

Dependant claim 17 includes the features of dependent claim 16 along with the additional feature of at least one of a web visiting card and emergency ID, stored on the

Internet via an authentication device, which contain the pseudonym ID (Page 4, paragraph 0013).

Dependant claim 18 includes the features of independent claim 1 along with the additional feature that the network is the internet (Page 7, paragraph 0026; Figure 1).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-4, 6, 7, 10-13 and 18 are rejected under the first paragraph of 35 U.S.C. 102(e) as being anticipated by Erickson et al. (U.S 2004/0199781).

Claims 5, 8, 9 and 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Erickson et al. (U.S. 2004/0199781) in view of Nagle et al. (U.S. 7181017).

VII. ARGUMENT

Erickson does not anticipate the present claimed invention and Erickson and Nagle when taken alone or in combination do not make the present claimed invention unpatentable. Thus, reversal of the Final Rejection (hereinafter termed "rejection") of claims 1-18 under 35 U.S.C. § 102(e) and 35 U.S.C. § 103(a) is respectfully requested.

Overview of the Cited References

Erickson et al. describe "a de-identification method and an apparatus for performing same on electronic datasets". Input datasets or databases that contain records relating to individual entities are processed to produce a resulting output dataset that contains as much information as possible while minimizing the risk that any individual in the input dataset could be re-identified from the output dataset. Individual entities may include patients in a hospital or be served by an insurance carrier, as well as voters, subscribers, customers, companies, or any other organization using discrete records. Criteria for preventing re-identification can be selected based on intended use of the output data and can be adjusted based on the content of reference databases. The method and system can also be associated with data acquisition equipment, such as a biologic data sampling device, to prevent de-identification of patient or other confidential data acquired by the equipment. (see Abstract).

Nagle describe a "system and method for communicating information between a first party and a second party". The method including identifying desired information, negotiating, through an intermediary, a comprehension function for obscuring at least a portion of the information communicated between the first party and the second party. The encrypted information is communicated to the second party and the encrypted information is decrypted using the negotiated comprehension function. Preferably, the intermediary does not itself possess sufficient information to decrypt the encrypted information, thus allowing use of an "non-trusted" intermediary. The comprehension function may be dynamic with respect to its response to the negotiated comprehension function, and thus permit limitations on the use of the information by the second party. For example, the decryption of the encrypted information may be time limited. (see Abstract).

Rejection of claims 1-4, 6, 10-13 and 18 under U.S.C. 102(e) as being anticipated by Erickson et al. (U.S 2004/0199781)

Reversal of the rejection of claims 1-4, 6, 10-13 and 18 under 35 U.S.C. 102(e) as being anticipated by Erickson et al. (U.S 2004/0199781) is respectfully requested because the rejection makes crucial errors in interpreting the cited reference. The rejection erroneously states that claims 1-4, 6, 7, 10-13 and 18 are anticipated by Erickson et al.

CLAIMS 1, 2, 10 and 18

Independent claim 1 recites "a personal electronic web health log for personal health data associated with a user, comprising: a data interface, usable to set up a communication link to system participants when required in order to transfer data from a local health log to system participants at least intermittently, wherein said local health log is included on a user's computer with pre-structured electronic forms for inputting the personal health data by system participants; and a converter for producing anonymous encrypted data permitting no inference of an identity of the user and for communicating said anonymous encrypted data addressed filing of at least a portion of said anonymous encrypted data on a network, said converter being actuated using selection schemes, including filters, said filters are valid for particular questions associated with said local health log and for marking data in the local health log used for targeted partial forwarding to system participants". For the reasons presented below, Erickson fails to provide any 35 USC 112 compliant enabling disclosure of each feature claimed in the present invention.

Unlike the claimed arrangement, Erickson describes a de-identification method and an apparatus for de-identifying particular electronic datasets. In Erickson, the datasets that contain records relating to individual entities are processed to produce a resulting output dataset that contains as much as information as possible while minimizing the risk that any individual in the input dataset could be re-identified from that output dataset (see Abstract of Erickson). However, contrary to the assertion by the Rejection, Erickson do not teach or suggest the above-identified features of the present invention.

For example, unlike the present invention, Erickson neither discloses nor suggests "a personal electronic web health log for personal health data associated with a user" as in the present invention. The claimed system provides each user the ability to enter, store and encrypt personal data for transmission to other users in the system. Erickson provides no enabling disclosure of the claimed features. Instead, Erickson merely describes a system for processing datasets that are input to the system by an operator wherein the datasets contain records relating to individual entities. The "individual entities may include patients in a hospital or served by an insurance carrier, votes, subscribers..." (see Page 1, paragraph 0011 of Erickson). Also, Erickson uses a k-anonymity analysis for truncating information in individual fields of the records to ensure the privacy of the individuals . Therefore, information related to or identifying any individual may be deleted in the interests of anonymization. Thus, the objective of Erickson is to provide data privacy assurance in the application to the statistical and bioinformatic arts (Page 1, Paragraph 0003). In other words, Erickson is directed to statistical data concerning records relating to many individuals within the "centralized" datasets. This is fundamentally different from a personal web health log for each respective individual user as in the present claimed invention. Thus, Erickson neither teach nor suggest "a personal electronic web health log for personal health data associated with a user" as recited in the present claimed invention.

Furthermore, the Rejection contends that Erickson, in paragraphs 0011, 0040, 0044, 0045, 0050, 0052, and 0054, teach or suggest "a data interface, usable to set up a communication link to system participants when required in order to transfer data from a local health log to system participants at least intermittently, wherein said local health log is included on a user's computer with pre-structured electronic forms for inputting the personal health data" as claimed in the present invention. The Rejection then asserts that these claimed features are being interpreted as an interface that allows users to input data. Applicant respectfully disagrees.

The present invention provides a data interface for setting up a communication link to system participants by transferring data from a local health log to system participants. The present invention also allows the local health log to be included on a user's computer (client-end) with pre-structured electronic forms for inputting personal data by the individual user. With this configuration, each user is able to enter, store, and encrypt personal data on their own respective computer. Then when required, the data from the local health log is transferred to other users via the data interface. One of the benefits of the present invention is that the "data [is] collated personally only with and by the user, so that it is not possible to relate the personal data and the anonymous data without the user or his records or his way of access" (Page 10, paragraph 0039 of Specification). In contrast, Erickson teaches away from the present invention in that an operator is responsible for inputting and storing records of many individuals into centralized datasets. In the system of Erickson, any user who has the authority will have access to all of the information from datasets. Only after the operator enters the records is the personal information excised from the record. Thus, contrary to the assertions by the Rejection, Erickson fails to disclose or suggest "a data interface, usable to set up a communication link to system participants when required in order to transfer data from a local health log to system participants at least intermittently, wherein said local health log is included on a user's computer with pre-structured electronic forms..." as recited in claim 1 of the present invention.

Additionally, Erickson describes a system employing a "k-anonymity analysis of abstract to produce a new data set that protects patient privacy, while providing as much information as possible from the original data set" (paragraph 0021). The system employs "a process algorithm that will identify fields within individual records that, if deleted ('scrubbed'), will result in k-anonymity for that dataset" (paragraph 0022). In other words, and unlike the present claimed system, Erickson allows persons other than the user to have access to all of the information from all datasets prior to the k-anonymity algorithm truncating information necessary for de-identification of a given record within the datasets. This is fundamentally different from the present invention which provides a user the ability to store personal information on a local health log maintained on the user's computer and uses a converter to encrypt the information prior to sharing it. Thus, Erickson neither discloses nor suggests "a personal electronic web health log for personal health data associated with a user...wherein said local health log is included on a user's computer...a converter for producing anonymous encrypted data permitting no inference of an identity of the user and for communicating said anonymous encrypted data addressed filing of at least a portion of said anonymous encrypted data on a network" as recited in claim 1 of the present invention.

Moreover, contrary to the Erickson system, the present invention provides selection schemes including filters which are valid for particular questions associated with elements of the local health log and which mark those data in the local health log which are important in this regard for targeted partial forwarding to system participants. The present invention provides this to limit doctors or others from gaining information of the user not pertinent to them. For example, "such schemes can effect subdivision such that they assign the data to respective appropriate medical areas, with the result that it is possible to make a data selection which comprises all the facts which are of interest to an internist or else the data for the optician or for an orthopedist" (Page 6, paragraph 0025 of Specification). Also, if a certain doctor is seeing a patient (the user of the personal web health log), the doctor may only mark particular information in the local health log used for targeted partial forwarding to system participants. In contrast, Erickson merely describes a k-anonymity analysis for truncating information in individual fields of the records result in a risk to the privacy of the persons who are the subject of the individual records. In the Erickson system, information relates to any individual and the information may be scrubbed in the interests of anonymization. There is no mechanism for filtering the data by a converter whereby the "filters are valid for particular questions" enabling "targeted partial forwarding" to others. Thus, Erickson neither teach nor suggest "said converter being actuated using selection schemes, including filters, said filters are valid for particular questions associated with said local health log and for marking data in the local health log used for targeted partial forwarding to system participants" as recited in claim 1 of the present invention. Consequently, Erickson fails to disclose each feature claimed in the present claimed invention and therefore does not anticipate the present claimed system.

In view of the above remarks, it is respectfully submitted that Erickson does not anticipate the present invention as claimed in independent claim 1. As claims 2, 10 and 18, are dependent on claim 1, they are considered to be patentable for the reasons given above with respect to claim 1. Consequently, withdrawal of the rejection of claims 1, 2, 10 and 18 is respectfully requested.

CLAIM 3

Dependent claim 3 is dependent on independent claim 1 and thus is patentable for the reasons presented above regarding claim 1. Additionally, claim 3 is considered patentable because Erickson fails to provide 35 USC 112 compliant enabling disclosure that the "user interface includes at least one of a keyboard and at least one interfaces to at least one of a card and label readers and a remote controller". While Erickson fail to disclose these features as recited in claim 3, the Rejection simply took official notice that the concept of inputting data into a system using a keyboard or card reader is old and well known in the art. Applicants traverse the official notice, and respectfully request that a proper prior art be cited to support this notion. Applicants respectfully request that the Rejection provide support for the assertion and explain how it may be combined with Erickson. Consequently, it is respectfully requested that the rejection of claim 3 be withdrawn.

CLAIM 4

Dependent claim 4 is dependent on independent claim 1 and thus is patentable for the reasons presented above regarding claim 1. Additionally, claim 4 is considered patentable because Erickson fails to disclose or suggest that "the local health log includes tables with chronological updating, free text fields and link elements". The present claimed invention provides link elements that allow jumps to other places in the local health log, other documents and Internet addresses (Page 5, paragraph 0019). Contrary to the assertion by the Rejection, the linking of remote databases in Erickson is not equivalent to the link elements of the present claimed invention which enable jumping to a specific location within a particular health record. The databases linked in Erickson enable access to multiple sources of data for a user to obtain that relates to already anonymized patient data. Also, there is no reason or motivation for Erickson to include this feature as the operation of the feature is solely related to the "local health log" which is "included on a user's computer" and not used in a centralized datasets environment such as the one described in Erickson. Thus, there is no 35 USC 112 compliant enabling disclosure in Erickson of the claimed feature in claim 4. Consequently, it is respectfully requested that the rejection of claim 4 be withdrawn.

CLAIM 6

Dependent claim 6 is dependent on independent claim 1 and thus is patentable for the reasons presented above regarding claim 1. Additionally, claim 6 is considered patentable because Erickson fails to disclose or suggest that "the selection schemes include elements of a consistency check for the purpose of checking the data for obvious errors and inconsistencies". The present claimed invention provides "selection schemes" including filters which are valid for particular questions associated with elements of the local health log and which mark those data in the local health log which are important in this regard for targeted partial forwarding to system participants. As discussed above, Erickson does not disclose or suggest such selection schemes as in the present invention. The data check performed by the claimed system ensures that the personal electronic web health log is free of obvious errors and inconsistencies. Erickson does not provide any mechanism to address the problem of erroneous or inconsistent data as in the present claimed invention. Thus, Erickson neither teach nor suggest "wherein the selection schemes include elements of a consistency check for the purpose of checking the data for obvious errors and inconsistencies" as recited in claim 6 of the present claimed invention. Consequently, it is respectfully requested that the rejection of claim 6 be withdrawn.

CLAIM 7

Dependent claim 7 is dependent on independent claim 1 and thus is patentable for the reasons presented above regarding claim 1. Claim 7 is also considered patentable because Erickson fails to disclose or suggest that "at least one anonymous encrypted health log is downstream of the converter, and is positioned at a storage location on the Internet via an Internet interface, and in which names and communication data for doctors are suppressed as standard and discriminating at least one of illnesses and treatments are suppressed at the responsibility of the user". The Rejection cites paragraphs 13, 32 and 55 as providing enabling disclosure of the feature claimed in claim 7. Applicant respectfully disagrees. In fact, the cited sections make no mention at all of "names and communication data for doctors" being suppressed and enabling a user to discriminate, "at least one of illness and treatments". Erickson is wholly concerned with removing data from to anonymize data but preserve the clinical information. Contrary to Erickson, the invention claimed in claim 7 enables a user to discriminate the data incorporated in the anonymous health log stored downstream from the converter. Erickson would not seek to incorporate the feature of "discriminating" by at least one of "illness or treatment" because Erickson is merely a system to remove information from records that could personally identify the patient associated with that record. Consequently, withdrawal of the rejection of claim 7 is respectfully requested.

CLAIM 11

Dependent claim 11 is dependent on independent claim 1 and thus is patentable for the reasons presented above regarding claims 1 and 2. Additionally, claim 11 is considered patentable because Erickson fails to disclose or suggest that "the local health log includes tables with chronological updating, free text fields and link elements". The present claimed invention provides link elements that allow jumps to other places in the local health log, other documents and Internet addresses (Page 5, paragraph 0019). Contrary to the assertion by the Rejection, databases that are linked together in Erickson are not equivalent to the claimed link elements. Also, there is no reason for Erickson to include this feature as the operation of the feature is solely related to the "local health log" which is "included on a user's computer" and not used in a centralized datasets environment such as the one described in Erickson. Thus, there is no 35 USC 112 compliant enabling disclosure in Erickson of the claimed feature in claim 11. Consequently, it is respectfully requested that the rejection of claim 11 be withdrawn.

CLAIM 12

Dependent claim 12 is dependent on independent claim 1 and thus is patentable for the reasons presented above regarding claims 1 and 3. Additionally, claim 12 is considered patentable because Erickson fails to disclose or suggest that "the local health log includes tables with chronological updating, free text fields and link elements". The present claimed invention provides link elements that allow jumps to other places in the local health log, other documents and Internet addresses (Page 5, paragraph 0019). Contrary to the assertion by the Rejection, databases that are linked together in Erickson are not equivalent to the claimed link elements. Also, there is no reason for Erickson to include this feature as the operation of the feature is solely related to the "local health log" which is "included on a user's computer" and not used in a centralized datasets environment such as the one described in Erickson. Thus, there is no 35 USC 112 compliant enabling disclosure in Erickson of the claimed feature in claim 12. Consequently, it is respectfully requested that the rejection of claim 12 be withdrawn.

CLAIM 13

Independent claim 13 recites "A personal electronic web health log for personal health data associated with a user". The web health log includes a data interface, usable to set up a communication link to system participants and adapted to transfer data from the health log to the system participants at least intermittently. The web health log also includes a user computer having at least a local health log with pre-structured electronic forms for inputting the personal health data and a converter. The converter produces anonymous encrypted data permitting no inference of an identity of the user and communicates the anonymous encrypted data addressed filing of at least a portion of the anonymous encrypted data on a network. The converter is adapted to be actuated using selection schemes, including filters. The filters are valid for particular questions associated with the local health log and for making data in the local health log used for targeted partial forwarding to system participants

For the reasons presented below, Erickson fails to provide any 35 USC 112 compliant disclosure of each feature claimed in claim 13. Erickson, unlike the present claimed invention, describes a de-identification method and an apparatus for performing same on electronic datasets. The datasets that contain records relating to individual entities are processed to produce a resulting output dataset that contains as much as information as possible while minimizing the risk that any individual in the input dataset could be re-identified from that output dataset (see Abstract of Erickson). However, contrary to the assertion by the Rejection, Erickson does not teach or suggest the above-identified features of the present invention.

For example, unlike the present invention, Erickson neither discloses nor suggests "a personal electronic web health log for personal health data associated with a user" as in the present invention. The claimed system provides each user the ability to enter, store and encrypt personal data for transmission to other users in the system. Erickson provides no enabling disclosure of the claimed features. Instead, Erickson merely describes a system processing datasets that are inputted to the system by an operator and the datasets contain records relating to individual entities. The "individual entities may include patients in a hospital or served by an insurance carrier, votes, subscribers…" (see Page 1, paragraph 0011 of Erickson). Also, Erickson uses a k-anonymity analysis for truncating information in individual fields of the records to ensure the privacy of the individuals . Therefore, information related to or identifying any individual may be scrubbed in the interests of anonymization. Thus, the objective of Erickson is to provide data privacy assurance in the application to the statistical and bioinformatic arts (Page 1, Paragraph 0003). In other words, Erickson is directed to statistical data of records relating to many individuals within a "centralized" dataset. This is fundamentally different from a personal web health log for each of individual users as in the present claimed invention. Thus, Erickson neither teach nor suggest "a personal electronic web health log for personal health data associated with a user" as recited in the present claimed invention.

Furthermore, the Rejection contends that Erickson, in paragraphs 0011, 0040, 0044, 0045, 0050, 0052, and 0054, teach or suggest "a data interface, usable to set up a communication link to system participants and adapted to transfer data from the health log to system participants at least intermittently, a user computer including, at least a local health log with pre-structured electronic forms for inputting the personal health data" as claimed in the present invention. The Rejection then asserts that these claimed features are being interpreted as an interface that allows users to input data. Applicant respectfully disagrees.

The present invention provides a data interface for setting up a communication link to system participants by transferring data from a local health log to system participants. The present invention also allows the local health log to be included on a user's computer (client-end) with pre-structured electronic forms for inputting personal data. With this configuration, each user is able to enter, store, and encrypt personal data on user's computer. Then when required, the data from the local health log is transferred to other users via the data interface. One of the benefits of the present invention is that the "data are collated personally only with and by the user, so that it is not possible to relate the personal data and the anonymous data without the user or his records or his way of access" (Page 10, paragraph 0039 of Specification). In contrast, Erickson teaches away from the present invention that an operator is responsible for inputting and storing records of many individuals into centralized datasets. In the system of Erickson, any user who has the authority will have access to all of the information from datasets. Thus, contrary to the assertions by the Rejection, Erickson neither teach nor suggest "a data interface, usable to set up a communication link to system participants and adapted to transfer data from the health log to system participants at least intermittently, a user computer including, at least a local health log with pre-structured electronic forms..." as recited in claim 13 of the present invention.

Additionally, Erickson describes a system employing a "k-anonymity analysis of abstract to produce a new data set that protects patient privacy, while providing as much information as possible from the original data set" (paragraph 0021). The system employs "a process algorithm that will identify fields within individual records that, if deleted ('scrubbed'), will result in k-anonymity for that dataset" (paragraph 0022). In other words, because the system of Erickson allows any user who has the authority to have access to all of the information from datasets, the pre-truncated information is available to persons other than the user until the k-anonymity algorithm truncates information necessary for de-identification of a given record within the given dataset. This is fundamentally different from the present invention which provides a user the ability to store personal information on a local health log maintained on the user's computer and then uses a converter to encrypt the information prior to sharing it. Thus, Erickson neither teach nor suggest "a personal electronic web health log for personal health data associated with a user…a user computer including at least a local health log…a converter, for producing anonymous encrypted data permitting no inference of an identity of the user and for communicating said anonymous encrypted data addressed filing of at least a portion of said anonymous encrypted data on a network" as recited in claim 13 of the present invention.

Moreover, contrary to Erickson et al, the present invention provides selection schemes including filters which are valid for particular questions associated with elements of the local health log and which mark those data in the local health log which are important in this regard for targeted partial forwarding to system participants. The present invention provides this to limit doctors or others from gaining information of the user not pertinent to them. For example, "such schemes can effect subdivision such that they assign the data to respective appropriate medical areas, with the result that it is possible to make a data selection which comprises all the facts which are of interest to an internist or else the data for the optician or for an orthopedist" (Page 6, paragraph 0025 of Specification). Also, if a certain doctor is seeing a patient (the user of the personal web health log), the doctor may only mark particular information in the local health log used for targeted partial forwarding to system participants. In contrast, Erickson merely describe a k-anonymity analysis for truncating information in individual fields of the records result in a risk to the privacy of the persons who are the subject of the individual records. In the system of Erickson, information relates to any individual may be scrubbed in the interests of anonymization. Thus, Erickson neither teach nor suggest "said converter is adapted to be actuated using selection schemes, including filters, said filters are valid for particular questions associated with said local health log and for marking data in the local health log used for targeted partial forwarding to system participants" as recited in claim 13 of the present invention.

In view of the above remarks, it is respectfully submitted that Erickson does not anticipate the present invention as claimed in independent claim 13. It is thus further respectfully submitted that this rejection is satisfied and should be withdrawn.

Rejection of claims 5, 8, 9 and 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Erickson et al. (U.S. 2004/0199781) in view of Nagle et al. (U.S. 7181017)

Reversal of the rejection of claims 5, 8, 9 and 14-17 under 35 U.S.C. 103(a) as being unpatentable over Erickson et al. (U.S. 2004/0199781) in view of Nagle et al. (U.S. 7181017) is respectfully requested because the rejection makes crucial errors in interpreting the cited references. The rejection erroneously states that claims 5, 8, 9 and 14-17 are made unpatentable by Erickson in view of Nagle et al.

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596, 1598 (Fed.Cir. 1988). In so doing, the Examiner is expected to make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (CCPA 1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion, or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed.Cir. 1988), *cert. denied*, 488 U.S. 825 (1988); *Ashland Oil Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 28, 293, 227 USPQ 657, 664 (Fed.Cir. 1985), *cert. denied*, 475 U.S. 1017 (1986); *ACS Hosp. Sys., Inc. v. Montefiore Hosp.*, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed.Cir. 1984). These showings by the Examiner are an essential part of complying with the burden of presenting a *prima facie* case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed.Cir. 1992).

CLAIM 5

Dependent claim 5 includes the features of claim 1 and therefore is considered patentable for the reasons presented above with respect to claim 1. Claim 5 is also considered patentable due to the additional feature that the link elements, which allow jumps to other places in the local health log, other documents and Internet addresses, include at least one of, link elements for charts and images, link elements for fax and photo reproductions and e-mails containing documents and connections to doctors, laboratories having further data.

Nagle describe a system and method for communicating information between a first party and a second party. Desired information is identified, negotiated, through an intermediary. A comprehension function obscures at least a portion of the information communicated between the first and the second party. The encrypted information is communicated to the second party and encrypted information is decrypted using the negotiated comprehension function. However, Nagle are not concerned with providing a personal electronic web health log for personal health data associated with a user. Thus, similarly to Erickson, Nagle neither discloses nor suggests "a personal electronic web health log for personal health data associated with a user, comprising: a data interface, usable to set up a communication link to system participants when required in order to transfer data from a local health log to system participants at least intermittently, wherein said local health log is included on a user's computer with pre-structured electronic forms for inputting the personal health data by system participants; and a converter for producing anonymous encrypted data permitting no inference of an identity of the user and for communicating said anonymous encrypted data addressed filing of at least a portion of said anonymous encrypted data on a network, said converter being actuated using selection schemes, including filters, said filters are valid for particular questions associated with said local health log and for marking data in the local health log used for targeted partial forwarding to system participants" as recited in independent claim 1 of the present claimed invention.

Furthermore, as admitted by the Rejection, Erickson fails to disclose or suggest links to data such as charts and emails. The Rejection then asserts that Nagel, in Col. 3, lines 31-34, teach or suggest the claimed feature of link elements for charts and images, link elements for fax and photo reproductions and e-mails containing documents and connections to doctors, laboratories having further data as in the present invention. Applicant respectfully disagrees. The relied upon portion of Nagel merely describes that the medical information includes different file types. File types are not equivalent to links to specific places in a local user health log as in the claimed invention. Thus, similarly to Erickson, Nagel neither discloses nor suggests "link elements, which allow jumps to other places in the local health log, other documents and Internet addresses, include at least one of, link elements for charts and images, link elements for fax and photo reproductions and e-mails containing documents and connections to doctors, laboratories having further data" as recited in claim 5 of the present claimed invention.

Additionally, there is no reason or suggestion to combine the Erickson system with the Nagle system because the combined system results in a central or intermediary system that governs how information is communicated as well as what subsets of the information is communicated to which parties. This is fundamentally different from the claimed system wherein each user is responsible for entering data in a personal health log on their computer system which may be filtered by requesting parties such that there is a targeted partial transmission of only the relevant data in the personal health log. Thus, the claimed system entirely removes the possibility that non-relevant information will be transmitted. Contrary to the claimed system the combined Erickson and Nagle system use an intermediary which selects which information is to be communicated, thus, to some degree, any and all information (relevant or not) is available to persons other than the user. Thus, the combined Erickson and Nagle system neither discloses nor suggest the claimed invention. Consequently, withdrawal of the rejection of claim 5 under 35 USC 103(a) is respectfully requested.

CLAIMS 8, 9 AND 14-17

Dependent claims 8, 9 and 14-17 includes the features of claims 1 and 13 respectively and therefore is considered patentable for the reasons presented above with respect to claims 1 and 13. Consequently, withdrawal of the rejection of claims 8, 9 and 14-17 under 35 USC 103(a) is respectfully requested.

VIII CONCLUSION

Erickson and Nagel et al. when taken alone or in combination, neither disclose nor suggest "a personal electronic web health log for personal health data associated with a user, comprising: a data interface, usable to set up a communication link to system participants when required in order to transfer data from a local health log to system participants at least intermittently, wherein said local health log is included on a user's computer with pre-structured electronic forms for inputting the personal health data by system participants; and a converter for producing anonymous encrypted data permitting no inference of an identity of the user and for communicating said anonymous encrypted data addressed filing of at least a portion of said anonymous encrypted data on a network, said converter being actuated using selection schemes, including filters, said filters are valid for particular questions associated with said local health log and for marking data in the local health log used for targeted partial forwarding to system participants" as recited in independent claim 1 of the present claimed invention" as recited in claim 1 and similarly in claim 13 of the present claimed invention.

Accordingly it is respectfully submitted that the rejection of Claims 1-18 should be reversed.

Respectfully submitted,
Siemens AG

Date: September 20, 2007

Alexander J. Burke
Reg. No. 40,425

Alexander J. Burke
Siemens Corporation,
Customer No. 28524
Tel. 732 321 3023
Fax 732 321 3030

APPENDIX I - APPEALED CLAIMS

1. (Previously Presented) A personal electronic web health log for personal health data associated with a user, comprising:

a data interface, usable to set up a communication link to system participants when required in order to transfer data from a local health log to system participants at least intermittently, wherein said local health log is included on a user's computer with pre-structured electronic forms for inputting the personal health data by system participants; and

a converter for producing anonymous encrypted data permitting no inference of an identity of the user and for communicating said anonymous encrypted data addressed filing of at least a portion of said anonymous encrypted data on a network, said converter being actuated using selection schemes, including filters, said filters are valid for particular questions associated with said local health log and for marking data in the local health log used for targeted partial forwarding to system participants.

2. (Previously Presented) The web health log as claimed in claim 1, wherein a user interface, protected by an authentication device, is for inputting and maintaining data.

3. (Previously Presented) The web health log as claimed in claim 2, wherein the user interface includes at least one of a keyboard and at least one interfaces to at least one of a card and label readers and a remote controller.

4. (Previously Presented) The web health log as claimed in claim 1, wherein the local health log includes tables with chronological updating, free text fields and link elements.

5. (Previously Presented) The web health log as claimed in claim 4, wherein the link elements, which allow jumps to other places in the local health log, other documents and Internet addresses, include at least one of,

link elements for charts and images,

link elements for fax and photo reproductions and e-mails containing documents and connections to doctors, laboratories having further data.

6. (Previously Presented) The web health log as claimed in claim 1, wherein the selection schemes include elements of a consistency check for the purpose of checking the data for obvious errors and inconsistencies.

7. (Previously Presented) The web health log as claimed in claim 1, wherein at least one anonymous encrypted health log is downstream of the converter, and is positioned at a

storage location on the Internet via an Internet interface, and in which names and communication data for doctors are suppressed as standard and discriminating at least one of illnesses and treatments are suppressed at the responsibility of the user.

8. (Previously Presented) The web health log as claimed in claim 1, further comprising a secure device for filing and finding a pseudonym ID under which the data are filed in encrypted form on the Internet.

9. (Previously Presented) The web health log as claimed in claim 8, further comprising at least one of a web visiting card and emergency ID, stored on the Internet via an authentication device, which contain the pseudonym ID.

10. (Previously Presented) The web health log as claimed in claim 1, further comprising a contractual module for transactions on a consumer-oriented health market.

11. (Previously Presented) The web health log as claimed in claim 2, wherein the local health log includes tables with chronological updating, free text fields and link elements.

12. (Previously Presented) The web health log as claimed in claim 3, wherein the local health log includes tables with chronological updating, free text fields and link elements.

13. (Previously Presented) A personal electronic web health log for personal health data associated with a user, comprising:

a data interface, usable to set up a communication link to system participants and adapted to transfer data from the health log to the system participants at least intermittently;

a user computer including,

at least a local health log with pre-structured electronic forms for inputting the personal health data,

and a converter, for producing anonymous encrypted data permitting no inference of an identity of the user and for communicating said anonymous encrypted data addressed filing of at least a portion of said anonymous encrypted data on a network, said converter is adapted to be actuated using selection schemes, including filters, said filters are valid for particular questions associated with said local health log and for making data in the local health log used for targeted partial forwarding, to system participants.

14. (Previously Presented) The web health log as claimed in clam 2, further comprising a secure device for filing and finding a pseudonym ID under which the data are filed in encrypted form on the Internet.

15. (Previously Presented) The web health log as claimed in claim 14, further comprising at least one of a web visiting card and emergency ID, stored on the Internet via an authentication device, which contain the pseudonym ID.

16. ({Previously Presented) The web health log as claimed in claim 3, further comprising a secure device for filing and finding a pseudonym ID under which the data are filed in encrypted form on the Internet.

17. (Previously Presented) The web health log as claimed in claim 16, further comprising at least one of a web visiting card and emergency ID, stored on the Internet via an authentication device, which contain the pseudonym ID.

18. (Previously Presented) The web health log as claimed in claim 1, wherein the network is the internet.

APPENDIX II - EVIDENCE

Applicants do not rely on any additional evidence other than the arguments submitted hereinabove.

APPENDIX III - RELATED PROCEEDINGS

Applicants respectfully submit that there are no proceedings related to this appeal in which any decisions were rendered.

APPENDIX IV - TABLE OF CASES

1. *In re Howard*, 394 F. 2d 869, 157 USPQ 615, 616 (CCPA 1968)
2. 29 AM. Jur 2D Evidence S. 33 (1994)
3. *In re Ahlert*, 424 F. 2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970)
4. *In re Eynde*, 480 F. 2d 1364, 1370; 178 USPQ 470, 474 (CCPA 1973)
5. *In re Fine*, 5 USPQ 2d 1600, (Fed Cir. 1988)
6. ACS Hospital Systems Inc v. Montefiore Hospital, 221 USPQ 929,933 (Fed. Cir. 1984)
7. *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (CCPA 1966)
8. *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed.Cir. 1988), *cert. denied*, 488 U.S. 825 (1988)
9. *Ashland Oil Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 28, 293, 227 USPQ 657, 664 (Fed.Cir. 1985), *cert. denied,* 475 U.S. 1017 (1986)
10. *In re Oetiker*, 977 F2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992)

APPENDIX V - LIST OF REFERENCES

U.S. Patent / Publication . No.	**Issued/ Publication Date**	**102(e) Date**	**Inventors**
2004/0199781	Oct. 7, 2004		Erickson et al.
7,181,017	Feb. 20, 2007		Nagel et al.

TABLE OF CONTENTS

ITEMS PAGE

I. Real Party in Interest 2

II. Related Appeals and Interferences 2

III. Status of Claims 2

IV. Status of Amendments 2

V. Summary of the Claimed Subject Matter 2-5

VI. Grounds of Rejection to be Reviewed on Appeal 5

VII. Argument 5-16

VIII Conclusion 17-18

APPENDICES

I. Appealed Claims 19-21

II. Evidence 22

III. Related Proceedings 23

IV. List of Cases 24

V. List of References 24